PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-007234
(43)Date of publication of application : 11.01.2002

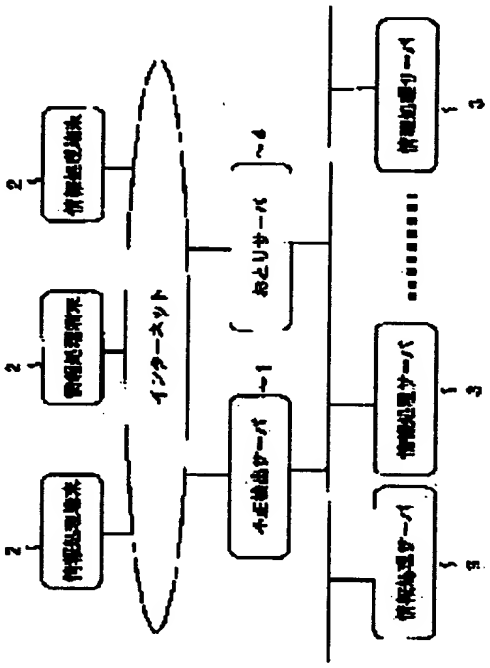
(51)Int.Cl. G06F 13/00
H04L 12/22

(21)Application number : 2000-184315
(22)Date of filing : 20.06.2000

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : OGOSHI TAKEHIRO

(54) DETECTION DEVICE, COUNTERMEASURE SYSTEM, DETECTING METHOD, AND COUNTERMEASURE METHOD FOR ILLEGAL MESSAGE, AND COMPUTER-READABLE RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To judge that illegal access is detected from information itself included in a packet, to intentionally let an illegal request source trespass, to deliberately make the trespasser think that the access has been successful, and to gather information (object of access, address of trespasser, procedure, etc.), regarding the illegal action meanwhile.
SOLUTION: An illegality detecting server 1 receiver packets sent from an information processor 2 to an information processing server 3 as the transmission destination, analyzes information included in the received packets to detect a packet having an illegal purpose, adds a mark representing the illegal packet to the illegal packet, and sends them to an information-processing server 3, having a function of deciding the marker or an undercover server 4; and the information processing server 3 or undercover server 4 having received the illegal packet with the added mark performs the processing to avoid illegality, such as the transmission of false information to the information processing terminal 2 which has sent the illegal packet.



BEST AVAILABLE COPY

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－7234
（P2002－7234A）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ　11/26		５Ｋ０３０

審査請求　未請求　請求項の数24　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－184315(P2000－184315)

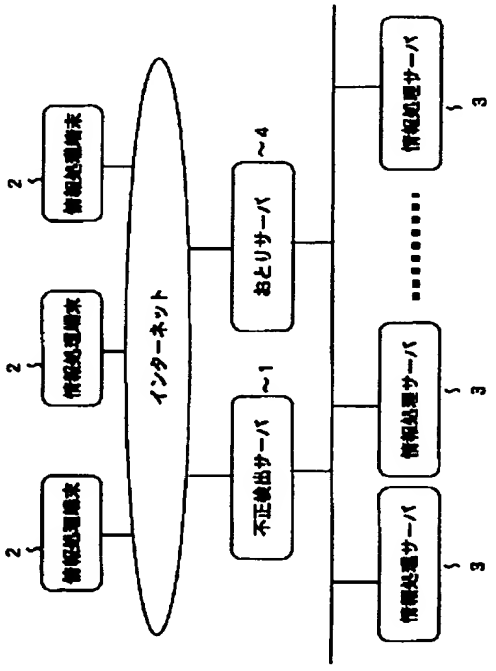
(22)出願日　平成12年６月20日(2000.6.20)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　大越　丈弘
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外２名）

Ｆターム(参考)　5B089 GA11 GA19 GB02 KA17 KC47
5K030 GA15 LC13 LE11

(54)【発明の名称】　不正メッセージ検出装置、不正メッセージ対策システム、不正メッセージ検出方法、不正メッセージ対策方法、及びコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　不正アクセスの検知をパケットに含まれる情報自体から判断し、不正な要求元に対してわざと侵入させ、侵入者には成功したと思わせておき、その間に不正に関する情報（アクセスの対象、侵入者のアドレス、手順等）を収集することを目的とする。
【解決手段】　情報処理サーバ３を送信先として情報処理端末２より送信されたパケットを不正検出サーバ１が受信し、不正検出サーバ１は受信したパケットに含まれる情報を分析して不正な目的を有するパケットを検出し、不正パケットであることを表示するマークを検出した不正パケットに付加し、マークを判別する機能を有する情報処理サーバ３又はおとりサーバ４に送信し、マークが付加された不正パケットを受信した情報処理サーバ３又はおとりサーバ４は、不正パケットを送信した情報処理端末２に対して偽情報を送信する等の不正回避処理を行う。



BEST AVAILABLE COPY

1

【特許請求の範囲】

【請求項１】　第一の情報処理装置と第二の情報処理装置とに接続され、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、

受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出装置であって、

前記第一の情報処理装置から送信された前記メッセージを受信する通信手段と、

前記通信手段により受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出手段とを有することを特徴とする不正メッセージ検出装置。

【請求項２】　前記不正メッセージ検出手段は、前記通信手段により受信された前記メッセージが特定のコマンドを含むか否かを分析することにより、前記不正メッセージを検出することを特徴とする請求項１に記載の不正メッセージ検出装置。

【請求項３】　前記不正メッセージ検出手段は、特定のコマンドを含む前記メッセージが前記通信手段により所定期間内に所定の個数以上受信されたか否かを分析することにより、前記不正メッセージを検出することを特徴とする請求項１に記載の不正メッセージ検出装置。

【請求項４】　前記不正メッセージ検出装置は、更に、不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出手段により検出された前記不正メッセージに付加する不正メッセージ表示情報付加手段を有することを特徴とする請求項１に記載の不正メッセージ検出装置。

【請求項５】　前記通信手段は、前記第一の情報処理装置より受信した前記メッセージを前記第二の情報処理装置へ送信し、

前記通信手段が前記第二の情報処理装置へ送信する前記メッセージには、前記不正メッセージ表示情報付加手段により前記不正メッセージ表示情報が付加された前記不正メッセージが含まれることを特徴とする請求項４に記載の不正メッセージ検出装置。

【請求項６】　前記不正メッセージ検出装置は、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理装置と接続されており、

前記通信手段は、前記不正メッセージ検出手段により検出された前記不正メッセージを、前記不正処理回避処理装置へ送信することを特徴とする請求項１に記載の不正メッセージ検出装置。

【請求項７】　前記通信手段は、前記不正メッセージ検出手段により検出された前記不正メッセージを、前記不正メッセージを送信した前記第一の情報処理装置へ送信することを特徴とする請求項１に記載の不正メッセージ検出装置。

2

【請求項８】　前記不正メッセージ検出装置は、更に、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理手段を有することを特徴とする請求項１に記載の不正メッセージ検出装置。

【請求項９】　前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、

前記不正処理回避処理手段は、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、

前記通信手段は、前記不正処理回避処理手段により作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする請求項８に記載の不正メッセージ検出装置。

【請求項１０】　第一の情報処理装置から送信されたメッセージを受信する第二の情報処理装置と、

前記第一の情報処理装置と前記第二の情報処理装置とに接続され、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出装置とを有する不正メッセージ対策システムであって、

前記不正メッセージ検出装置は、

前記第一の情報処理装置から送信された前記メッセージを受信し、受信した前記メッセージを前記第二の情報処理装置へ送信する通信手段と、

前記通信手段により受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出手段と、

不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出手段により検出された前記不正メッセージに付加する不正メッセージ表示情報付加手段とを有し、

前記通信手段が前記第二の情報処理装置へ送信する前記メッセージには、前記不正メッセージ表示情報付加手段により前記不正メッセージ表示情報が付加された前記不正メッセージが含まれ、

前記第二の情報処理装置は、

前記不正メッセージ検出装置より送信された前記メッセージを受信し、受信した前記メッセージに対する応答を前記第一の情報処理装置へ送信する送受信手段と、

前記不正メッセージに付加された前記不正メッセージ表示情報を検出することにより、前記送受信手段により受信された前記メッセージから前記不正メッセージを判別する不正メッセージ判別手段と、

前記不正メッセージが目的とする不正処理を回避する処

理である不正処理回避処理を行う不正処理回避処理手段とを有することを特徴とする不正メッセージ対策システム。

【請求項１１】　前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、

前記第二の情報処理装置の前記不正処理回避処理手段は、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、

前記第二の情報処理装置の前記送受信手段は、前記不正処理回避処理手段により作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする請求項１０に記載の不正メッセージ検出装置。

【請求項１２】　第一の情報処理装置と第二の情報処理装置とに接続され、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出装置と、

前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理装置とを有する不正メッセージ対策システムであって、

前記不正メッセージ検出装置は、

前記第一の情報処理装置から送信された前記メッセージを受信し、受信した前記メッセージのうち前記不正メッセージを前記不正処理回避処理装置へ送信する通信手段と、

前記通信手段により受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出手段とを有し、

前記不正処理回避処理装置は、

前記不正メッセージ検出装置より送信された前記不正メッセージを受信し、前記不正メッセージに対する応答を前記不正メッセージを送信した前記第一の情報処理装置へ送信する送受信手段と、

前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理手段とを有することを特徴とする不正メッセージ対策システム。

【請求項１３】　前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、

前記不正処理回避処理装置の前記不正処理回避処理手段は、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、

前記不正処理回避処理装置の前記送受信手段は、前記不正処理回避処理手段により作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする請求項１２に記載の不正メッセージ検出装置。

【請求項１４】　第一の情報処理装置と第二の情報処理装置との間で通信を行い、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、

受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法であって、

前記第一の情報処理装置から送信された前記メッセージを受信する通信ステップと、

前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップとを有することを特徴とする不正メッセージ検出方法。

【請求項１５】　前記不正メッセージ検出方法は、更に、

不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出ステップにより検出された前記不正メッセージに付加する不正メッセージ表示情報付加ステップを有することを特徴とする請求項１４に記載の不正メッセージ検出方法。

【請求項１６】　前記通信ステップは、前記第一の情報処理装置より受信した前記メッセージを前記第二の情報処理装置へ送信し、

前記通信ステップが前記第二の情報処理装置へ送信する前記メッセージには、前記不正メッセージ表示情報付加ステップにより前記不正メッセージ表示情報が付加された前記不正メッセージが含まれることを特徴とする請求項１５に記載の不正メッセージ検出方法。

【請求項１７】　前記不正メッセージ検出方法は、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理装置と通信を行い、

前記通信ステップは、前記不正メッセージ検出ステップにより検出された前記不正メッセージを、前記不正処理回避処理装置へ送信することを特徴とする請求項１４に記載の不正メッセージ検出方法。

【請求項１８】　第一の情報処理方法から送信されたメッセージを受信する第二の情報処理方法と、

前記第一の情報処理方法と前記第二の情報処理方法との間で通信を行い、前記第二の情報処理方法を送信先として前記第一の情報処理方法から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理方法に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法とを有する不正メッセージ対策方法であって、

前記不正メッセージ検出方法は、
前記第一の情報処理方法から送信された前記メッセージを受信し、受信した前記メッセージを前記第二の情報処理方法へ送信する通信ステップと、
前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップと、
不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出ステップにより検出された前記不正メッセージに付加する不正メッセージ表示情報付加ステップとを有し、
前記通信ステップが前記第二の情報処理方法へ送信する前記メッセージには、前記不正メッセージ表示情報付加ステップにより前記不正メッセージ表示情報が付加された前記不正メッセージが含まれ、
前記第二の情報処理方法は、
前記不正メッセージ検出方法より送信された前記メッセージを受信し、受信した前記メッセージに対する応答を前記第一の情報処理方法へ送信する送受信ステップと、
前記不正メッセージに付加された前記不正メッセージ表示情報を検出することにより、前記送受信ステップにより受信された前記メッセージから前記不正メッセージを判別する不正メッセージ判別ステップと、
前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理ステップとを有することを特徴とする不正メッセージ対策方法。

【請求項１９】　前記第二の情報処理方法に対し、前記第二の情報処理方法が有する情報を前記不正メッセージを送信した前記第一の情報処理方法へ送信することを、前記不正メッセージが要求する場合に、
前記第二の情報処理方法の前記不正処理回避処理ステップは、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、
前記第二の情報処理方法の前記送受信ステップは、前記不正処理回避処理ステップにより作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理方法に送信することを特徴とする請求項１８に記載の不正メッセージ検出方法。

【請求項２０】　第一の情報処理装置と第二の情報処理装置との間で通信を行い、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法と、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理方法とを有する不正メッセージ対策方法であって、前記不正メッセージ検出方法は、

前記第一の情報処理装置から送信された前記メッセージを受信し、受信した前記メッセージのうち前記不正メッセージを前記不正処理回避処理方法へ送信する通信ステップと、
前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップとを有し、前記不正処理回避処理方法は、
前記不正メッセージ検出方法より送信された前記不正メッセージを受信し、前記不正メッセージに対する応答を前記不正メッセージを送信した前記第一の情報処理装置へ送信する送受信ステップと、
前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理ステップとを有することを特徴とする不正メッセージ対策方法。

【請求項２１】　前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、
前記不正処理回避処理方法の前記不正処理回避処理ステップは、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、
前記不正処理回避処理方法の前記送受信ステップは、前記不正処理回避処理ステップにより作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする請求項２０に記載の不正メッセージ検出方法。

【請求項２２】　第一の情報処理装置と第二の情報処理装置との間で通信を行い、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、
受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法であって、
前記第一の情報処理装置から送信された前記メッセージを受信する通信ステップと、
前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップとを有することを特徴とする不正メッセージ検出方法を、
コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２３】　前記コンピュータ読み取り可能な記録媒体は、
前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理手段を有することを特徴とする不正メッセージ検出方法を、
コンピュータに実行させるためのプログラムを記録した

請求項２２に記載のコンピュータ読み取り可能な記録媒体。

【請求項２４】　前記コンピュータ読み取り可能な記録媒体は、

前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、

前記不正処理回避処理ステップは、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、

前記通信ステップは、前記不正処理回避処理ステップにより作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする不正メッセージ検出方法を、

コンピュータに実行させるためのプログラムを記録した請求項２３に記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンピュータネットワークシステムに悪い影響をおよぼす可能性のあるメッセージが含まれるパケットのコンピュータネットワークシステムへの侵入を検知する不正メッセージ検出装置に関する。

【０００２】

【従来の技術】図５は例えば、特開平９－２６６４７５に示された従来のアドレス情報管理装置及びネットワークシステムであり、パケットの送信元のアドレスから不正アクセスか否か判断しようとするものである。図５において、５１はアドレス情報管理装置ＬＥＣＳ１、５２は不正な侵入先であるＬＥＳ２、５３は侵入対策用端末、５４は不正な要求元である。

【０００３】次に動作について説明する。図において、不正な要求元５４がＬＥＣＳ１に対してＬＥＳ２のアドレスを要求する。ＬＥＣＳ１は要求パケットの発信元アドレスが、あらかじめ格納してあるアドレステーブルにあるか否か検査する。発信元アドレスがあらかじめ設定されている値の範囲に合致してない場合、この要求が不正な使用者によるものであると判断し、ＬＥＳ２ではなく侵入対策用端末５３のアドレスを通知する。

【０００４】

【発明が解決しようとする課題】従来の侵入検知方式では、不正メッセージを有するパケットか否かの判断を、パケットの送信元のアドレスを用いて、あらかじめ設定されている値か否かで判断していた。そのため、不正を行う侵入者が正式な要求元からアクセスする場合、不正な侵入であるにもかかわらず、不正なパケットであると判断できず、侵入されてしまう。

【０００５】また、不正な侵入にもいろいろな方法があり、当然のことながらその検知の仕方にもいろいろある。代表的なものとして、システムのセキュリティホールを利用したコマンドの送信、必要以上にサイズの大きなデータの送信、通常の運用では発生しない一定間時間内の大量の接続要求等のアクセスがある。これらの攻撃は、システムの稼動を妨害し、システムが正常に動作しなくなるだけでなく、システム内にある機密情報の漏洩等、システムを利用している組織にとって多大な影響を及ぼすことになる。送信元があらかじめ設定されていたものであるか否かで不正か否かを判断する従来の方式では、不正なパケットを、不正であると認識できないという問題点があった。

【０００６】この発明は上記のような問題点を解決するためになされたもので、不正アクセスの検知をパケットの要求元ではなくパケットに含まれる情報自体から判断し、不正な要求元に対してわざと侵入させ、侵入者には成功したと思わせておき、その間に不正に関する情報（アクセスの対象、侵入者のアドレス、手順等）を収集することを目的とする。

【０００７】

【課題を解決するための手段】この発明に係る不正メッセージ検出装置は、第一の情報処理装置と第二の情報処理装置とに接続され、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出装置であって、前記第一の情報処理装置から送信された前記メッセージを受信する通信手段と、前記通信手段により受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出手段とを有することを特徴とする。

【０００８】前記不正メッセージ検出手段は、前記通信手段により受信された前記メッセージが特定のコマンドを含むか否かを分析することにより、前記不正メッセージを検出することを特徴とする。

【０００９】前記不正メッセージ検出手段は、特定のコマンドを含む前記メッセージが前記通信手段により所定期間内に所定の個数以上受信されたか否かを分析することにより、前記不正メッセージを検出することを特徴とする。

【００１０】前記不正メッセージ検出装置は、更に、不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出手段により検出された前記不正メッセージに付加する不正メッセージ表示情報付加手段を有することを特徴とする。

【００１１】前記通信手段は、前記第一の情報処理装置より受信した前記メッセージを前記第二の情報処理装置へ送信し、前記通信手段が前記第二の情報処理装置へ送

信する前記メッセージには、前記不正メッセージ表示情報付加手段により前記不正メッセージ表示情報が付加された前記不正メッセージが含まれることを特徴とする。

【００１２】前記不正メッセージ検出装置は、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理装置と接続されており、前記通信手段は、前記不正メッセージ検出手段により検出された前記不正メッセージを、前記不正処理回避処理装置へ送信することを特徴とする。

【００１３】前記通信手段は、前記不正メッセージ検出手段により検出された前記不正メッセージを、前記不正メッセージを送信した前記第一の情報処理装置へ送信することを特徴とする。

【００１４】前記不正メッセージ検出装置は、更に、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理手段を有することを特徴とする。

【００１５】前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、前記不正処理回避処理手段は、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、前記通信手段は、前記不正処理回避処理手段により作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする。

【００１６】第一の情報処理装置から送信されたメッセージを受信する第二の情報処理装置と、前記第一の情報処理装置と前記第二の情報処理装置とに接続され、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出装置とを有する不正メッセージ対策システムであって、前記不正メッセージ検出装置は、前記第一の情報処理装置から送信された前記メッセージを受信し、受信した前記メッセージを前記第二の情報処理装置へ送信する通信手段と、前記通信手段により受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出手段と、不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出手段により検出された前記不正メッセージに付加する不正メッセージ表示情報付加手段とを有し、前記通信手段が前記第二の情報処理装置へ送信する前記メッセージには、前記不正メッセージ表示情報付加手段により前記不正メッセージ表示情報が付加された前記不正メッセージが含まれ、前記第二の情報処理装置は、前記不正メッセージ検出装置より送信された前記メッセージを受信し、受信した前記メッセージに対する応答を前記第一の情報処理装置へ送信する送受信手段と、前記不正メッセージに付加された前記不正メッセージ表示情報を検出することにより、前記送受信手段により受信された前記メッセージから前記不正メッセージを判別する不正メッセージ判別手段と、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理手段とを有することを特徴とする。

【００１７】前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、前記第二の情報処理装置の前記不正処理回避処理手段は、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、前記第二の情報処理装置の前記送受信手段は、前記不正処理回避処理手段により作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする。

【００１８】第一の情報処理装置と第二の情報処理装置とに接続され、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出装置と、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理装置とを有する不正メッセージ対策システムであって、前記不正メッセージ検出装置は、前記第一の情報処理装置から送信された前記メッセージを受信し、受信した前記メッセージのうち前記不正メッセージを前記不正処理回避処理装置へ送信する通信手段と、前記通信手段により受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出手段とを有し、前記不正処理回避処理装置は、前記不正メッセージ検出装置より送信された前記不正メッセージを受信し、前記不正メッセージに対する応答を前記不正メッセージを送信した前記第一の情報処理装置へ送信する送受信手段と、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理手段とを有することを特徴とする。

【００１９】前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、前記不正処理回避処理装置の前記不正処理回避処理手段は、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、前記不正処理回避処理装置の前記送受信手段は、前記不正処理回避処理手段により作成された前記偽

メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする。

【００２０】第一の情報処理装置と第二の情報処理装置との間で通信を行い、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法であって、前記第一の情報処理装置から送信された前記メッセージを受信する通信ステップと、前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップとを有することを特徴とする。

【００２１】前記不正メッセージ検出方法は、更に、不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出ステップにより検出された前記不正メッセージに付加する不正メッセージ表示情報付加ステップを有することを特徴とする。

【００２２】前記通信ステップは、前記第一の情報処理装置より受信した前記メッセージを前記第二の情報処理装置へ送信し、前記通信ステップが前記第二の情報処理装置へ送信する前記メッセージには、前記不正メッセージ表示情報付加ステップにより前記不正メッセージ表示情報が付加された前記不正メッセージが含まれることを特徴とする。

【００２３】前記不正メッセージ検出方法は、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理装置と通信を行い、前記通信ステップは、前記不正メッセージ検出ステップにより検出された前記不正メッセージを、前記不正処理回避処理装置へ送信することを特徴とする。

【００２４】第一の情報処理方法から送信されたメッセージを受信する第二の情報処理方法と、前記第一の情報処理方法と前記第二の情報処理方法との間で通信を行い、前記第二の情報処理方法を送信先として前記第一の情報処理方法から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理方法に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法とを有する不正メッセージ対策方法であって、前記不正メッセージ検出方法は、前記第一の情報処理方法から送信された前記メッセージを受信し、受信した前記メッセージを前記第二の情報処理方法へ送信する通信ステップと、前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップと、不正メッセージであることを表示する不正メッセージ表示情報を、前記不正メッセージ検出ステップにより検出された前記不正メッセージに付加する不正メッセージ表示情報付加ステップとを有し、前記通信ステップが前記第二の情報処理方法へ送信する前記メッセージには、前記不正メッセージ表示情報付加ステップにより前記不正メッセージ表示情報が付加された前記不正メッセージが含まれ、前記第二の情報処理方法は、前記不正メッセージ検出方法より送信された前記メッセージを受信し、受信した前記メッセージに対する応答を前記第一の情報処理方法へ送信する送受信ステップと、前記不正メッセージに付加された前記不正メッセージ表示情報を検出することにより、前記送受信ステップにより受信された前記メッセージから前記不正メッセージを判別する不正メッセージ判別ステップと、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理ステップとを有することを特徴とする。

【００２５】前記第二の情報処理方法に対し、前記第二の情報処理方法が有する情報を前記不正メッセージを送信した前記第一の情報処理方法へ送信することを、前記不正メッセージが要求する場合に、前記第二の情報処理方法の前記不正処理回避処理ステップは、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、前記第二の情報処理方法の前記送受信ステップは、前記不正処理回避処理ステップにより作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理方法に送信することを特徴とする。

【００２６】第一の情報処理装置と第二の情報処理装置との間で通信を行い、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法と、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理方法とを有する不正メッセージ対策方法であって、前記不正メッセージ検出方法は、前記第一の情報処理装置から送信された前記メッセージを受信し、受信した前記メッセージのうち前記不正メッセージを前記不正処理回避処理方法へ送信する通信ステップと、前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップとを有し、前記不正処理回避処理方法は、前記不正メッセージ検出方法より送信された前記不正メッセージを受信し、前記不正メッセージに対する応答を前記不正メッセージを送信した前記第一の情報処理装置へ送信する送受信ステップと、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理ステップとを有することを特徴とする。

【００２７】前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記

不正メッセージが要求する場合に、前記不正処理回避処理方法の前記不正処理回避処理ステップは、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、前記不正処理回避処理方法の前記送受信ステップは、前記不正処理回避処理ステップにより作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする。

【００２８】本発明は、第一の情報処理装置と第二の情報処理装置との間で通信を行い、前記第二の情報処理装置を送信先として前記第一の情報処理装置から送信されたメッセージを受信し、受信した前記メッセージから、前記第二の情報処理装置に不正処理を加えることを目的とする不正メッセージを検出する不正メッセージ検出方法であって、前記第一の情報処理装置から送信された前記メッセージを受信する通信ステップと、前記通信ステップにより受信された前記メッセージに含まれる情報を分析することにより、不正メッセージを検出する不正メッセージ検出ステップとを有することを特徴とする不正メッセージ検出方法を、コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

【００２９】前記コンピュータ読み取り可能な記録媒体は、前記不正メッセージが目的とする不正処理を回避する処理である不正処理回避処理を行う不正処理回避処理手段を有することを特徴とする不正メッセージ検出方法を、コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

【００３０】前記コンピュータ読み取り可能な記録媒体は、前記第二の情報処理装置に対し、前記第二の情報処理装置が有する情報を前記不正メッセージを送信した前記第一の情報処理装置へ送信することを、前記不正メッセージが要求する場合に、前記不正処理回避処理ステップは、前記不正メッセージの要求に応答するメッセージであって、前記不正メッセージの要求とは異なる情報を有する偽メッセージを作成し、前記通信ステップは、前記不正処理回避処理ステップにより作成された前記偽メッセージを、前記不正メッセージを送信した前記第一の情報処理装置に送信することを特徴とする不正メッセージ検出方法を、コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

【００３１】

【発明の実施の形態】実施の形態１．図１は、本実施の形態に係る不正メッセージ対策システムの構成図である。図１において、１は不正メッセージ検出装置である不正検出サーバである。不正検出サーバ１は、インターネット等のネットワークを経由して、情報処理端末２より、パケットを受信し、受信したパケットを分析する手段及び不正メッセージ表示情報たるマークを生成し、パケットにマークを付加する手段を保持する。そして、不正検出サーバ１は、マークが付加されたパケットを情報処理サーバ３に受け渡す。

【００３２】２は、インターネット等のネットワークに接続された第一の情報装置である情報処理端末であり、特定情報へのアクセス要求等のメッセージを情報処理サーバ３へ送信する。具体手的には、クライアントコンピュータ等の情報処理端末が該当する。

【００３３】３は、インターネット等のネットワークに接続された第二の情報処理装置である情報処理サーバであり、攻撃者又は侵入者による攻撃及び侵入の対象となる。情報処理サーバ３は、不正検出サーバ１によりマークが付加された不正パケットを処理する手段を装備している。情報処理サーバ３は、メールサーバ、ｆｔｐサーバ、ｈｔｔｐサーバ等であり、通常のパケット（不正処理の目的を持たないパケット）を受信している間は、通常のサーバとしての情報処理を行う。一方、不正検出サーバ１からマークが付加された不正パケットを受信すると、通常の処理は行わず、偽情報の応答といった不正処理回避処理を行う。

【００３４】図２は、不正検出サーバ１のモジュール構成を示す図である。図２において、１１は通信手段、１２は不正メッセージ検出手段たるパケット分析手段、１３は不正メッセージ表示情報付加手段たるマーク生成付加手段である。通信手段１１は、情報処理端末２から情報処理サーバ３を送信先として送信されたパケットを受信し、受信したパケットを情報処理端末２が送信先に指定した情報処理サーバ３へ送信する。また、不正なパケットを受信した場合には、マーク生成付加手段によりマークが付加されたパケットを３へ送信する。パケット分析手段１２は、通信手段１１が受信したパケットを分析し、不正パケットを検出する。不正パケットの検出は、パケットに含まれる情報自体を分析することにより行う。なお、具体的なパケット分析方法については後述する。マーク生成付加手段１３は、パケット分析手段１２により不正パケットと判断されたパケットに、不正メッセージ表示情報たるマークを付加する。

【００３５】図３は、情報処理サーバ３のモジュール構成を示す図である。図３において、３１は送受信手段たる通信手段であり、不正検出サーバ１よりパケットを受信し、またパケットに含まれるメッセージに応じて各種の情報を情報処理端末２へ送信する。３２は、不正メッセージ判別手段たるマーク判別手段であり、通信手段３１により受信されたパケットにマークが付加されているか否かの判断を行う。３３は、不正回避処理手段であり、マーク判別手段により不正パケットと判断された場合に、不正パケットを送信した情報処理端末に対して偽メッセージの送信等の不正処理回避処理を行う。

【００３６】次に動作について説明する。まず不正検出サーバ１は、通信手段１１により、情報処理端末から送信されたパケットを受信する。そして、パケット分析手段１２によりパケットが不正か否かを解析する。パケット分析手段１２によるパケット分析は、後に詳述するように、要求元のアドレスだけではなく、パケット内のデータ、コマンド、アクセスの頻度等によって判断する。次に、受信されたパケットが、パケット分析手段１２により不正であると判断された場合、マーク生成付加手段１３によりマークを生成し不正と判断されたパケットに付加する。不正パケットに対するマークの付加は、パケットのヘッダ又はデータ部に追加するだけではなく、電子透かしのようにパケット内に挿入させてもよい。そして、マーク生成付加手段１３により不正パケットにマークが付加された後、不正検出サーバ１は、通信手段１１を用いて送信先である情報処理サーバ３へ送信する。

【００３７】次に、情報処理サーバ３では、通信手段３１によりパケットを受信する。そして、マーク判別手段３２を用いて、受信したパケットにマークが付加されているか否かを判別することにより、受信したパケットが不正か否かを判別する。マークがない場合は、通常の処理を行う。マークがある場合、不正回避処理手段３３により、通常の処理を行わず偽情報等の応答をする。

【００３８】侵入者の特定には、１度や２度のパケットを分析しただけでは、侵入者の特定、侵入方法、システムの脆弱点・セキュリティホール等の侵入に関する情報を収集及び分析することは難しい。分析するパケットが多ければ多いほど、より有効な情報の入手及び分析が可能となる。上述したように、情報処理サーバ３は、偽情報の応答等の処理をすることにより、侵入者に侵入成功と思わせることができる。このため、侵入者に何度でも攻撃させて、侵入者のアドレス、侵入の方法・手順、時間帯といった、侵入に関するより有効な情報を収集することができるし、侵入者の特定・侵入に対する有功な対処策等の分析及び対策実施のための時間をとることができる。

【００３９】また、偽情報等の応答の仕方を、毎回変えてもよい。なぜならば、侵入に対して、同じ偽情報を毎回応答すると、侵入者に検知されていることを察知される可能性があるためである。なお、偽情報の変更は、定期的に行ってもよいし、不定期であってもよい。また、コマンドごとに変更する等により、侵入するごとに毎回同じ結果にならなければよい。

【００４０】次に、パケットの分析方法の例について説明する。パケットの分析方法には大きくわけると次の２つの方法で行う。

（１）パケット内に含まれている文字列やコードを検査するパターンマッチング

（２）一定時間に一定以上の個数のパケットを検知する統計的な手法

以下にて、（１）パターンマッチングによる手法の例を３つ、（２）統計的な手法の例を１つ示す。

【００４１】（パターンマッチング１）メールサーバへのバッファオーバーフロー攻撃の検知方法

この攻撃を受けると、メールサーバは、異常終了、誤動作等正常に動作しなくなる。この攻撃を検知するためには、パケットが以下のようなパターン（コマンド）になっているか否か分析する。

ＴＣＰヘッダ

Ｄｅｓｔｉｎａｔｉｏｎ Ｐｏｒｔ ＝ ２５（ＳＭＴＰであることを表す）ＴＣＰデータ

以下のｓｍｔｐコマンドの引数が１２８バイト以上か否かで判断する。

“ｈｅｌｏ”，“ｍａｉｌ ｆｒｏｍ：”，“ｒｃｐｔ ｔｏ：”，“ｖｒｆｙ”，“ｅｘｐｎ”

メールサーバへのバッファオーバーフロー攻撃は、実際には、ｐｏｐに対してもあり、上記は、あくまでも一例である。また、メールサーバへの攻撃には、ｓｍｔｐのコマンドを利用してユーザ名・ユーザの有無などの情報取得といったさまざまな攻撃が存在する。

【００４２】（パターンマッチング２）ＦＴＰ ＣＷＤ ～ｒｏｏｔ攻撃の検知方法

この攻撃を受けると、ｆｔｐサーバは、ルート権限を取得される。そのため、パスワードファイル等の重要なファイルが改ざん又は盗まれたり、ウイルス等の不正処理を行うプログラムをセットアップされ、実行されて、ｆｔｐサーバが正常に動作しなくなる可能性がある。この攻撃を検知するためには、パケットが以下のようなパターン（コマンド）になっているか否か分析する。

ＴＣＰヘッダ

Ｄｅｓｔｉｎａｔｉｏｎ Ｐｏｒｔ ＝ ２１（ＦＴＰ－ＣＯＮＴＲＯＬ）

ＴＣＰデータ

“ｃｗｄ ～ｒｏｏｔ”の文字列を検知する。

【００４３】（パターンマッチング３）ｈｔｔｐ ｐｈｆ のバグを用いた攻撃の検知方法

この攻撃を受けると、ｈｔｔｐサーバは、ルート権限でコマンドを実行されてしまう。そのため、パスワードファイル等の重要なファイルが改ざん又は盗まれたり、ウイルス等の不正処理を行うプログラムをセットアップされ、実行されて、ｈｔｔｐサーバが正常に動作しなくなる可能性がある。この攻撃を検知するためには、パケットが以下のようなパターン（コマンド）になっているか否か分析する。

ＴＣＰヘッダ

Ｄｅｓｔｉｎａｔｉｏｎ Ｐｏｒｔ ＝ ８０（ＨＴＴＰ）

ＴＣＰデータ

“ＧＥＴ△”，“／ＰＨＦ”（△はスペースをあらわす）の文字列を検知

【００４４】（統計的な手法１）ＳＹＮフラッド攻撃の検知方法
この攻撃をうけると、ＳＹＮパケット対応のためにリソースがなくなり、システムの負荷が高くなり、他のサービスを実行することができなくなる。この攻撃を検知するためには、一定時間内（例えば１０秒間）に、以下に該当するパケットが一定個数（例えば１００個）以上あるか否かを分析する。
ＩＰヘッダのＤｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓが共通
ＴＣＰヘッダのＳＹＮフラグが１、ＡＣＫフラグが０
【００４５】以上のように、不正か否かの判断を、要求元のアドレスだけではなく、パケット内のデータ、コマンド、アクセスの頻度等によって判断しているので、侵入者が正規な要求元から侵入しようとしても侵入を検知することができる。
【００４６】また、侵入者の特定には、１度や２度のパケットを分析しただけでは、侵入者の特定、侵入方法、システムの脆弱点・セキュリティホール等の侵入に関する情報を収集及び分析することは難しい。分析するパケットが多ければ多いほど、より有効な情報の入手及び分析が可能となる。本実施の形態では、偽情報の応答等の処理をすることにより侵入者に侵入成功と思わせることができるため、侵入者に何度でも攻撃させて、侵入者のアドレス、侵入の方法・手順、時間帯といった、侵入に関するより有効な情報を収集することができるし、侵入者の特定・侵入に対する有功な対処策等の分析及び対策実施のための時間をとることができる。
【００４７】また、不正パケットに対するマークの付加は、パケットのヘッダ又はデータ部に追加するだけではなく、電子透かしのようにパケット内に挿入させてもよい。このようにすることで、ヘッダ解析等のプロトコル処理の際に追加したマークが削除される可能性を回避できるし、また、実施の形態３において説明するように、マークを付加したまま応答を侵入者に返したとしても、侵入者に侵入を検知したことを気づかれないという効果がある。そのため、侵入が検知されているにもかかわらず、侵入者は攻撃を続ける。一回の不正パケットよりは、多くの不正パケットの方がより侵入に関する情報を収集することができる。上記のように、侵入者に侵入成功と思わせてしばらく攻撃させることにより、侵入に関する情報を収集可能となる。
【００４８】実施の形態２．以上の実施形態１では、情報処理サーバ３すべてにマーク判別手段３２、不正回避処理手段３３を実装するようにしたものであるが、次に、不正処理回避処理装置たるおとりサーバをネットワークに追加する実施形態を示す。
【００４９】図４は、本実施の形態に係る不正メッセージ対策システムの構成図である。図４において、４は、不正パケットが目的とする不正処理を回避する処理を専門的に行う、おとりサーバである。おとりサーバ４は、不正検出サーバ１から不正パケットを受信すると、偽情報の送信といった処理を行う。このため、おとりサーバ４も実施の形態１における情報処理サーバ３と同様の不正回避処理手段を有している。なお、図中の１～３は、実施の形態１と同様である。
【００５０】次に、動作について説明する。実施の形態１と同様に、不正検出サーバ１は、パケット分析手段１２により、受信したパケットが不正か否かを判断する。次に、受信したパケットが不正であると判断すると、不正検出サーバ１は、パケットで指定された送信先に関わらず、全て不正パケットをおとりサーバ４へ送信する。本実施の形態では、おとりサーバ４は不正パケットに対する処理を行う専用装置であるため、おとりサーバ４が受信するパケットはすべて不正パケットである。従って、本実施の形態では、不正検出サーバ１は、不正パケットにマークを付加することを要しない。
【００５１】次に、不正パケットを受信したおとりサーバ４は、実施の形態１と同様に、偽情報の応答、コマンド処理を行う。おとりサーバ４を用いると、ネットワーク内のすべての情報処理サーバの処理をカスタマイズする必要がないため、既存のシステムに侵入検知システムの導入のための改修作業を削減できる。また、偽情報等の応答の仕方を、毎回変えてもよい。なぜならば、侵入に対して、同じ偽情報を毎回応答すると、侵入者に検知されていることを察知される可能性があるため。なお、偽情報の変更は、定期的に行ってもよいし、不定期であってもよい。また、コマンドごとに変更する等により、侵入するごとに毎回同じ結果にならなければよい。
【００５２】なお、実施の形態では、負荷分散のためにもおとりサーバを独立した専用装置としたが、かならずしも専用装置とする必要はなく、通常は情報処理サーバとして機能し、不正パケットが送信された場合のみ、おとりサーバ４として機能する装置であってもよい。但し、この場合は、不正検出サーバ１において、不正パケットにマークを付加する処理を追加する必要がある。
【００５３】実施の形態３．実施の形態１及び実施の形態２においては、不正検出サーバ１は、パケットの送信先である情報処理サーバ３、又はおとりサーバ４に不正パケットを送信していたが、不正検出サーバ１は情報処理サーバ３又はおとりサーバ４に送信することなく、不正検出サーバ１自身が不正回避処理を行うことも可能である。即ち、図２に示した不正検出サーバ１のモジュール構成に加え、不正回避処理手段を設けることにより、不正検出サーバ１自身が偽情報の送信等の不正パケットに対する対策を実施することができる。
【００５４】実施の形態４．実施の形態１及び実施の形態２では、不正検出サーバ１は不正パケットを検知すると、不正回避処理手段を備えた装置（情報処理サーバ３又はおとりサーバ４）にパケットを送信していたが、お

とりサーバ、情報処理サーバにパケットを送信せずに、要求元である情報処理端末２へ中継してもよい。要求元である情報処理端末２へ中継することにより、侵入者に侵入成功と思わせておく。そして、侵入者が、侵入先（実は、侵入者自身）からパスワードファイル、システムファイル等の重要な情報を盗もうとした場合、不正パケットを中継した装置は、侵入者の重要な情報を入手することができ、対策のための重要な情報を入手することができる。また、侵入者が侵入先（実は、侵入者自身）のシステムを動作不能にする攻撃を実施する場合、侵入者自身を攻撃することになるため、侵入者が攻撃の対象としていたネットワークシステムはシステムの動作不能となることなく攻撃を回避することができる。

【００５５】以上のように、不正侵入対策システムに用いられる、本発明に係る不正検知装置は、以下の手段を備えている。コンピュータネットワークシステムにおいて、以下の手段を備えたことを特徴とする。

（ａ）通信手段

（ｂ）受信したパケットの内容を解析して不正か否かを判断するパケット分析手段

（ｃ）不正なパケットに、不正であることを表すマークをパケットに付加するマーク生成付加手段

【００５６】また、不正侵入対策システムに用いられる、本発明に係る情報処理装置は、以下のの手段を備えている。

（ａ）通信手段

（ｂ）受信したパケットに、不正であることを表すマークが付加されているか否かを検出するマーク検出手段

（ｃ）不正パケットであった場合、パケットの内容によって、偽情報の送信等の偽の応答をして、侵入者に侵入成功と思わせる対策実施手段

【００５７】また、不正侵入対策システムに用いられる、本発明に係る不正検知手段は、受信したパケットが不正であると判断した場合、要求元にパケットを中継するための手段を備えたことを特徴とする。

【００５８】更に、不正侵入対策システムに用いられる、本発明に係る情報処理装置は、侵入者に応答するための偽情報を変更又は生成するための手段を備えたことを特徴とする。

【００５９】

【発明の効果】以上のように、本発明によれば、不正検出サーバは、パケットの内容自体で不正であるか否かを判断するため、正規な要求元から送信された不正なパケットであっても検出することができ、正規の要求元からの攻撃を検知できるという効果がある。

【００６０】また、本発明によれば、不正検出サーバは、不正なパケットを表示するマークを不正なパケットに付加するため、情報処理サーバは不正なパケットを判別することができ、適切な不正処理回避処理を行うことができる。

【００６１】更に、本発明によれば、情報処理サーバは、不正なパケットに対して偽情報の応答等の不正処理回避処理を行うことにより、不正に関する情報の収集及び分析をより有効なものにすることができる。

【００６２】更に、本発明によれば、不正回避処理を行うおとりサーバを設けたため、ネットワーク内のすべての情報処理装置の処理をカスタマイズする必要がなく、既存のシステムに侵入検知システムの導入のための改修作業、コストを削減できる。

【００６３】また、本発明によれば、不正検出サーバ自身に不正処理回避処理を行わせることができるため、既存のシステムに新たにおとりサーバを設ける必要がなく、改修作業、コストを削減できる。

【００６４】また、本発明によれば、不正検出サーバは、不正パケットを要求元に中継することにより、侵入者の攻撃回避するとともに侵入者の情報を入手することができる。

【００６５】また、偽情報を変えることにより、侵入者に侵入検知を諭されることを防ぐことができる。

【図面の簡単な説明】

【図１】　この発明の一実施の形態を示す全体構成図。

【図２】　不正検出サーバのモジュール構成を示す図。

【図３】　情報処理サーバのモジュール構成を示す図。

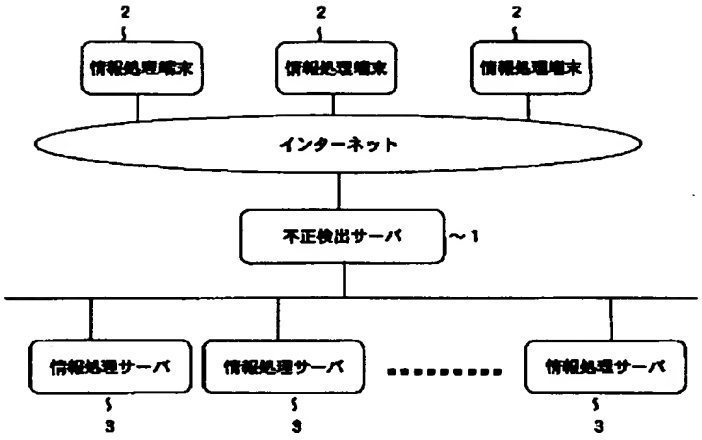
【図４】　この発明の実施の形態２を示す全体構成図。

【図５】　従来技術を示す構成図。

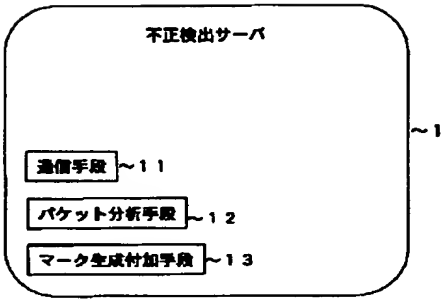
【符号の説明】

１　不正検出サーバ、２　情報処理端末、３　情報処理サーバ、４　おとりサーバ、１１　通信手段、１２　パケット分析手段、１３　マーク生成付加手段、３１　通信手段、３２　マーク判別手段、３３　不正回避処理手段。

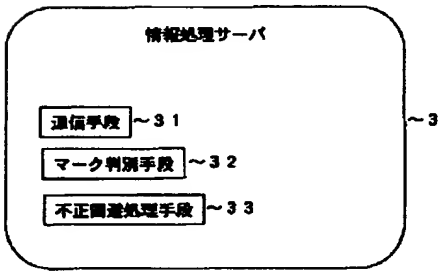
【図１】



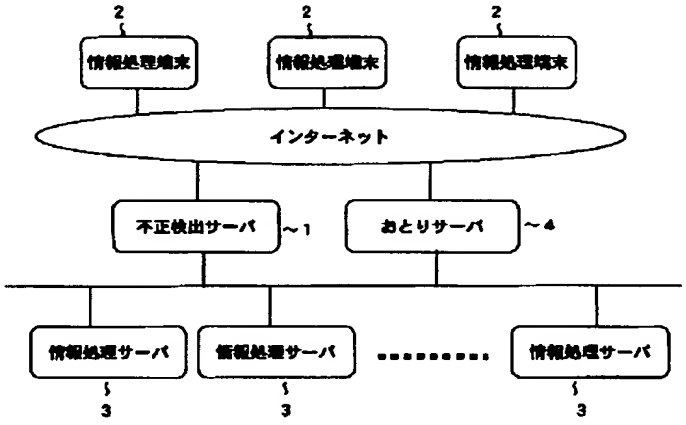
【図２】



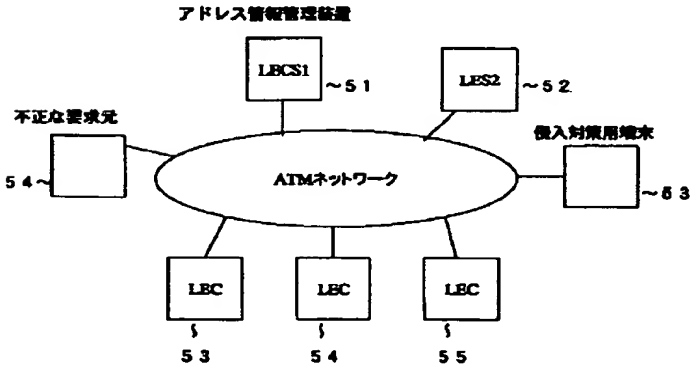
【図３】



【図４】



【図５】



BEST AVAILABLE COPY